Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	33	(James near Vogt).in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L2	66	(Robert near Hasbun).in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L3	9	(John near Brizek).in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L4	100	L1 or L2 or L3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L5	74727	flash adj (memory or array)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L6	65143	(unauthoriz$4 or protect$3 or hidden or lock$4) near2 (area or section)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L7	893	L5 and L6	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L8	167	bad near password$2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08
L9	3	L7 and L8	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:08

L10	395	invalid adj2 password	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:11
L11	48923	count$4 same ((invalid adj2 password) or attempt$2 or fail$4 or (unauthoriz$4 adj2 access$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:14
L12	21450	count$4 with ((invalid adj2 password) or attempt$2 or fail$4 or (unauthoriz$4 adj2 access$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:17
L13	23	(((authenticat$3 or password or passcode or keycode) near3 valid) and (flash adj (memory or array))) and (memory adj2 bank$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:15
L14	1	12 and 13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:15
L15	24930	"711"/$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 12:17
L16	387	12 and 15	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 13:23
L17	2	"5469564".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/05/27 13:23

Terms used
unauthorized access counter counters invalid passwords authentication flash eeprom hidden storage

Fc
8,15
155

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Data integrity: Web application security assessment by fault injection and behavior monitoring

Yao-Wen Huang, Shih-Kun Huang, Tsung-Po Lin, Chung-Hung Tsai

May 2003 **Proceedings of the 12th international conference on World Wide Web**

Full text available: pdf(4.53 MB) Additional Information: full citation, abstract, references, citings, index terms

As a large and complex application platform, the World Wide Web is capable of delivering a broad range of sophisticated applications. However, many Web applications go through rapid development phases with extremely short turnaround time, making it difficult to eliminate vulnerabilities. Here we analyze the design of Web application security assessment mechanisms in order to identify poor coding practices that render Web applications vulnerable to attacks such as SQL injection and cross-site scr ...

Keywords: black-box testing, complete crawling, fault injection, security assessment, web application testing

2 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004 **Proceedings of the 41st annual conference on Design automation - Volume 00**

Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

***Keywords**: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

3 Illustrative risks to the public in the use of computer systems and related technology

Peter G. Neumann

January 1996 **ACM SIGSOFT Software Engineering Notes**, Volume 21 Issue 1

Full text available: pdf(2.54 MB) Additional Information: full citation

4 A taxonomy of computer program security flaws

Carl E. Landwehr, Alan R. Bull, John P. McDermott, William S. Choi

September 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 3

Full text available: pdf(3.81 MB) Additional Information: full citation, abstract, references, citings, index terms, review

An organized record of actual flaws can be useful to computer system designers, programmers, analysts, administrators, and users. This survey provides a taxonomy for computer program security flaws, with an Appendix that documents 50 actual security flaws. These flaws have all been described previously in the open literature, but in widely separated places. For those new to the field of computer security, they provide a good introduction to the characteristics of security flaws and how they ...

Keywords: error/defect classification, security flaw, taxonomy

5 Unlinkable serial transactions: protocols and applications

Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag

November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

6 Reflection as a mechanism for software integrity verification

Diomidis Spinellis

February 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 1

Full text available: pdf(85.99 KB) Additional Information: full citation, abstract, references, index terms, review

The integrity verification of a device's controlling software is an important aspect of many emerging information appliances. We propose the use of reflection, whereby the software is able to examine its own operation, in conjunction with cryptographic hashes as a basis for developing a suitable software verification protocol. For more demanding applications meta-reflective techniques can be used to thwart attacks based on device emulation strategies. We demonstrate how our approach can be ...

Keywords: cryptographic hash function, embedded device, message digest

7 Data base directions: the next steps

John L. Berg

November 1976 , Volume 8 , 8 Issue 4 , 2

Full text available: pdf(9.95 MB) Additional Information: full citation, abstract

What information about data base technology does a manager need to make prudent decisions about using this new technology? To provide this information the National Bureau of Standards and the Association for Computing Machinery established a workshop of approximately 80 experts in five major subject areas. The five subject areas were auditing, evolving technology, government regulations, standards, and user experience. Each area prepared a report contained in these proceedings. The proceedings p ...

Keywords: DBMS, auditing, cost/benefit analysis, data base, data base management, government regulation, management objectives, privacy, security, standards, technology assessment, user experience

8 Securing a global village and its resources: baseline security for interconnected signaling system #7 telecommunications networks

Hank M. Kluepfel

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Full text available: pdf(1.19 MB) Additional Information: full citation, abstract, references, index terms

The resulting national focus on Network Integrity issues, spawned the development of an industry commitment to affect and realize a minimum security baseline for interconnected SS7 networks. In addition the affected carriers in those outage have accelerated their pursuit of secure solutions to today's intelligent networking.[2]This paper will focus on the development of the baseline and the current effort to take the baseline into national, e.g., National Ins ...

9 Enabling trusted software integrity

Darko Kirovski, Milenko Drinić, Miodrag Potkonjak

October 2002 **Proceedings of the 10th international conference on Architectural support for programming languages and operating systems**, Volume 37 , 30 , 36 Issue 10 , 5 , 5

Full text available: pdf(1.39 MB) Additional Information: full citation, abstract, references, citings

Preventing execution of unauthorized software on a given computer plays a pivotal role in system security. The key problem is that although a program at the beginning of its execution can be verified as authentic, while running, its execution flow can be redirected to externally injected malicious code using, for example, a buffer overflow exploit. Existing techniques address this problem by trying to detect the intrusion at run-time or by formally verifying that the software is not prone to a p ...

10 Strong password-only authenticated key exchange

David P. Jablon

October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

11 The information furnace: consolidated home control

Diomidis D. Spinellis

May 2003 **Personal and Ubiquitous Computing**, Volume 7 Issue 1

Full text available: pdf(488.36 KB) Additional Information: full citation, abstract, index terms

The Information Furnace is a basement-installed PC-type device that integrates existing consumer home-control, infotainment, security and communication technologies to transparently provide accessible and value-added services. A modern home contains a large number of sophisticated devices and technologies. Access to these devices is currently provided through a wide variety of disparate interfaces. As a result, end users face a bewildering array of confusing user-interfaces, access modes a ...

Keywords: Automation,.Consumer electronics, Home-control, Multi-modal interfaces

12 Protection and the control of information sharing in multics
Jerome H. Saltzer
July 1974 **Communications of the ACM**, Volume 17 Issue 7

Full text available: pdf(1.75 MB) Additional Information: full citation, abstract, references, citings, index terms

The design of mechanisms to control the sharing of information in the Multics system is described. Five design principles help provide insight into the tradeoffs among different possible designs. The key mechanisms described include access control lists, hierarchical control of access specifications, identification and authentication of users, and primary memory protection. The paper ends with a discussion of several known weaknesses in the current protection mechanism design.

Keywords: Multics, access control, authentication, computer utilities, descriptors, privacy, proprietary programs, protected subsystems, protection, security, time-sharing systems, virtual memory

13 Authentication and authorization: Securing passwords against dictionary attacks
Benny Pinkas, Tomas Sander
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

Full text available: pdf(216.72 KB) Additional Information: full citation, abstract, references, citings, index terms

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user' ...

14 Logical and physical design issues for smart card databases
Cristiana Bolchini, Fabio Salice, Fabio A. Schreiber, Letizia Tanca
July 2003 **ACM Transactions on Information Systems (TOIS)**, Volume 21 Issue 3

Full text available: pdf(1.12 MB) Additional Information: full citation, abstract, references, citings, index terms

The design of very small databases for smart cards and for portable embedded systems is deeply constrained by the peculiar features of the physical medium. We propose a joint approach to the logical and physical database design phases and evaluate several data structures with respect to the performance, power consumption, and endurance parameters of read/program operations on the Flash-EEPROM storage medium.

Keywords: Design methodology, access methods, data structures, flash memory, personal information systems, smart card

15 SIGCOMM 1- Software-hardware interactions: An experimental application of cryptography

to a remotely accessed data system
J. L. Smith, W. A. Notz, P. R. Osseck
August 1972 **Proceedings of the ACM annual conference - Volume 1**

Full text available: pdf(1.46 MB) Additional Information: full citation, abstract, references, citings

An experimental system has been developed which illustrates ways cryptography can be applied to certain data-security problems concerning remotely accessible data files. These problems are in two main classes: security of data while in transit over communications lines and security of data while in storage. The system makes use of a combination of software and special hardware to provide enciphering and deciphering of messages between a terminal and a data processor. Not only is the content of m ...

Keywords: communication security, cryptography, data communications, data security, data-base protection, file protection, teleprocessing, terminals authentication, time-shared systems

16 SPINS: security protocols for sensor networks
Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler
September 2002 **Wireless Networks**, Volume 8 Issue 5

Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

17 Revokable and versatile electronic money (extended abstract)
Markus Jakobsson, Moti Yung
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

18 Columns: Risks to the public in computers and related systems
Peter G. Neumann
July 2001 **ACM SIGSOFT Software Engineering Notes**, Volume 26 Issue 4

Full text available: pdf(1.17 MB) Additional Information: full citation

19 SPINS: security protocols for sensor netowrks
Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar
July 2001 **Proceedings of the 7th annual international conference on Mobile computing and networking**

Full text available: pdf(242.17 KB) Additional Information: full citation, abstract, references, citings, index terms

As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, much research has focused on making sensor networks feasible and useful, and has not concentrated on security.

We present a suite of security building blocks optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and &mgr;TESLA SNEP provides the following important baseline security primitives: Data confidentia ...

20 Technical trials and legal tribulations
Scott Craver, Boon-Lock Yeo, Minerva Yeung
July 1998 **Communications of the ACM**, Volume 41 Issue 7

Full text available: pdf(641.01 KB) Additional Information: full citation, references, citings, index terms, review

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next